Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1.-7. (Cancelled)

8. (Currently Amended) An authentication process involving a first ~~entity~~device, which possesses a public key v and a secret key s, the public and secret keys being related by an operation modulo n, where n is an integer, the modulus n being specific to the first ~~entity~~device, and a second ~~entity~~device, which knows the public key v, the first and second entities being provided with means to exchange zero-knowledge information and to carry out cryptographic calculations on the zero-knowledge information, calculations being carried out modulo n wherein in the process the modulo n operation is of $v=s^{-t} \pmod n$, t being a parameter and in that the modulo n calculations are performed according to the "Chinese remainders" method.

9. (Currently Amended) A process according to claim 8, wherein the information exchanges are of zero-knowledge and wherein the cryptographic calculations are completed as follows:

the first ~~entity~~device selects are at least one integer r at random ranging between 1 and n-1 and calculates at least one parameter x equal to $r^t \pmod n$, then at least one number c that is at least one function of the at least one of a parameter and a message and sends the at least one number c to the second ~~entity~~device;

the second ~~entity~~device receives the at least number c, selects at least one number e at random, and sends the at least one number e to the first ~~entity~~device;

the first ~~entity~~device receives the at least one number e, carries out at least one calculation using the at least one number e and the secret key s, the result of the at least one calculation yielding at least one answer y, and sends the at least one answer y to the second ~~entity~~device.

the second ~~entity~~device receives the at least one answer y, carries out one calculation using the public key v and the modulus n, and checks with a modulo n operation that the result of the one calculation is coherent with the received at least one number c.

10. (Previously Presented) A process according to Claim 9, wherein a size of the number n, expressed in number of bits, is less than 1,000.

11. (Previously Presented) A process according to Claim 10, wherein a size of the number n is between 700 and 800.

12. (Cancelled)

13. (Currently Amended) A message signature process configured for a ~~signatory~~device provided with a public key v and a secret key s, the public and private keys being related by a modulo n calculation, where n is an integer, which is specific to the ~~signatory~~device, the process utilizing means configured to calculate at least one number c that is a function of a message M to be signed, configured to calculate at least one number y that is a function of the secret key s, and configured to transmit the numbers y and c that are the signature of the message and the message M, wherein the modulo n operation is v=s-t (mod n), t being a parameter.

14. (Currently Amended) A message signature process according to claim 13, wherein the ~~signatory~~device selects an integer r at random between 1 and n-1, calculates a parameter x equal to rt (mod n), calculates at least one number e that is a function of parameter x and the message M to be signed, calculates the at least one number y using its secret key s, said at least one number y being a function of numbers r and e, and transmits the numbers c and y as the signature.